HIPAA - Privacy – Gov't Protection of Health Information

TRICARE Management Activity, Electronic Business Policy & Standards

January 2003
OSD(HA), TMA eBPS

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Highlights

HIPAA PROGRAM OFFICE

Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA
22041-3206
Ph: 703-681-5611
Fax: 703-681-8845

TMA HIPAA Website:
www.tricare.osd.mil/hipaa

E-Mail:
hipaamail@tma.osd.mil

TRICARE Management Activity

General Requirement

Under the Privacy Rule, government-operated health plans and health care providers must meet substantially the same requirements as private ones for protecting the privacy of individually identifiable health information (PHI). For instance, government-run health plans, such as Medicare and Medicaid, must take virtually the same steps to protect the claims and health information that they receive from beneficiaries as private insurance plans or health maintenance organizations (HMO). In addition, all federal agencies must also meet the requirements of the Privacy Act of 1974, which restricts what information about individual citizens - including any personal health information - can be shared with other agencies and with the public.

The only new authority for government involves enforcement of the Privacy Rule itself. In order to ensure covered entities protect patients' privacy as required, the rule provides that health plans, hospitals, and other covered entities cooperate with the Department's efforts to investigate complaints or otherwise ensure compliance. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the privacy protections and access rights for consumers under this rule.

Roles and Responsibilities of OCR

OCR has been assigned the responsibility of enforcing the Privacy Rule. As is typical in many enforcement settings, OCR may need to look at how a covered entity handled medical records and other personal health information. The Privacy Rule limits disclosure to OCR information that is "pertinent to ascertaining compliance." OCR will maintain stringent controls to safeguard any individually identifiable health information that it receives. If covered entities could avoid or ignore enforcement requests, consumers would not have a way to ensure an independent review of their concerns about privacy violations under the rule.

An important ingredient in ensuring compliance with the Privacy Rule is the responsibility of HHS to investigate complaints that the rule has been violated and to follow up on other information regarding noncompliance. At times, this responsibility entails seeing personal health information, such as when an individual indicates to HHS that they believe a covered entity has not properly handled its medical records.

What information would be needed depends on the circumstances and the alleged violations. The Privacy Rule limits OCR's access to information that is "pertinent to ascertaining compliance." In some cases, no personal health information would be needed. For instance, OCR may need to review only a business contract to determine whether a health plan included appropriate language to protect privacy when it hired an outside company to help process claims.

Examples of investigations that may require OCR to have access to PHI include:

- Allegations that a covered entity refused to note a request for correction in a patient's medical record, or did not provide complete access to a patient's medical records to that patient.
- Allegations that a covered entity used health information for marketing purposes without first obtaining the individuals' authorization when required by the rule. OCR may need to review information in the marketing department that contains personal health information, to determine whether a violation has occurred.

Access to Medical Information by Police and Law Enforcement Agencies

The rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists. Today, law enforcement officers obtain health information for many purposes, sometimes without a warrant or other prior process. The rule establishes new procedures and safeguards to restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant.

Even in those circumstances when disclosure to law enforcement is permitted by the rule, the Privacy Rule does not require covered entities to disclose any information. Some other federal or state law may require a disclosure, and the Privacy Rule does not interfere with the operation of these other laws. However, unless the disclosure is required by some other law, covered entities should use their professional judgment to decide whether to disclose information, reflecting their own policies and ethical principles. In other words, doctors, hospitals, and health plans could continue to follow their own policies to protect privacy in such instances.

Reporting a Communicable Disease to Public Health Authorities

All states have laws that require providers to report cases of specific diseases to public health officials. The Privacy Rule allows disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affected by a disease. In some cases they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting deaths and births, investigating the occurrence and cause of injury and disease, and monitoring adverse outcomes related to food, drugs, biological products, and dietary supplements.

Relationship with the Privacy Act

The Privacy Act of 1974 protects personal information about individuals held by the federal government. Covered entities that are federal agencies or federal contractors that maintain records that are covered by the Privacy Act not only must obey the HIPAA Privacy Rule's requirements but also must comply with the Privacy Act.